UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/771,591	02/04/2004	John M. Hayden	10830.0102.N	3791

27927 7590 06/06/2007

RICHARD AUCHTERLONIE
NOVAK DRUCE & QUIGG, LLP
1000 LOUISIANA
53RD FLOOR
HOUSTON, TX 77002

EXAMINER	
LOHN, JOSHUA A	
ART UNIT	**PAPER NUMBER**
2114	

MAIL DATE	DELIVERY MODE
06/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/771,591	HAYDEN ET AL.	
	Examiner	Art Unit	
	Joshua A. Lohn	2114	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *11-14 and 31-33* is/are allowed.

6)☒ Claim(s) *1-5,7-10,15-25,27-30 and 34-41* is/are rejected.

7)☒ Claim(s) *6 and 26* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/11/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5, 7, 10, 15, 18, 20, 21-25, 27, 30, 34, and 41 are rejected under 35 U.S.C. 102(e) as being anticipated by Witte et al., United States Patent number 7,143,307, filed March 15, 2002.

As per claim 1, Witte discloses *in a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site* (Witte, col. 2, lines 49-60), *the secondary virtual file server needing resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site* (Witte, col. 7, lines 54-60), *a method comprising:*

a) determining whether there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing user access at the disaster recovery site (Witte, col. 7, lines 47-51, where the backup filer acts as the virtual secondary file server, and col. 7, lines 52-60, where the created backup has reserved interfaces

and storage, which is functionally equivalent to file system mounts, the reservation inherently showing determination that sufficient resources exist); *and*

b) upon finding that there are sufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing user access at the disaster recovery site, reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site (Witte, col. 8, lines 19-25, where the reserving of interfaces and mounts occurs to maintain client access during disaster recovery).

As per claim 2, Witte further discloses *the method as claimed in claim 1, wherein the primary file server is a virtual file server* (Witte, col. 7, lines 52-56, where the filers. are the servers and are also virtual).

As per claim 3, Witte further discloses *the method as claimed in claim 1, which is performed when it is desired to perform a configuration change of the primary file server at the active site, and which includes performing a configuration change of the primary file server at the active site after reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site once the configuration change of the primary file server at the active site has been performed* (Witte, col. 12, lines 23-40, where the primary network configuration is changed once backup is created, which includes any reservations; this configuration change will allow user access to the backup, col. 12, 34-35).

As per claim 4, Witte further discloses *the method as claimed in claim 1, which is performed when it is desired to failover user access from the active site to the disaster recovery site, and which includes performing failover of user access from the active site to the disaster recovery site after reserving the network interfaces and file system mounts that are needed at the disaster recovery site for providing user access at the disaster recovery site after failover of user access from the active site to the disaster recovery site* (Witte, col. 12, lines 21-40).

As per claim 5, Witte further discloses *the method as claimed in claim 1, wherein user mappings are kept at the disaster recovery site so that user file access at the active site may be continued by accessing user file copies at the disaster recovery site upon failover of user access from the active site to the disaster recovery site* (Witte, col. 8, lines 1-11, where each filer includes user access mappings and these configurations are kept at the backup site, col. 11, lines 41-61).

As per claim 7, Witte further discloses *the method as claimed in claim 1, wherein user session information is kept at the disaster recovery site so that users accessing user files of the primary file server at the active site may access copies of the user files at the disaster recovery site without a need to log onto the disaster recovery site upon failover of user access from the active site to the disaster recovery site* (Witte, col. 12, lines 23-54, where the session information is maintained and the live version of data is available; the client user session need not log onto the disaster recovery site since all the access is automatically transferred).

As per claim 10, Witte further discloses *the method as claimed in claim 1, which includes the disaster recovery site producing and storing a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a consistent state for the secondary virtual file server* (Witte, col. 7, lines 8-20).

As per claim 15, Witte discloses *in a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site* (Witte, col. 2, lines 49-60), *the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site* (Witte, col. 7, lines 11-13), *a method comprising:*

maintaining a copy of user session information at the disaster recovery site during user file access at the active site; and

upon failover of user access from the primary file server at the active site to the virtual secondary server at the disaster recovery site, accessing the copy of the user session information at the disaster recovery site so that users accessing files of the primary file server at the active site continue to access copies of the files at the disaster recovery site without a need to log onto the disaster recovery site (Witte, col. 12, lines 23-54, where the session information is maintained and the live version of data is available; the client user session need not log onto the disaster recovery site since all the access is automatically transferred).

As per claim 18, Witte further discloses *the method as claimed in claim 15, which includes the disaster recovery site producing and storing a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a consistent state for the secondary virtual file server* (Witte, col. 7, lines 8-20).

As per claim 20, Witte discloses *in a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site* (Witte, col. 2, lines 49-60), *the primary file server storing a collection of user files, and the secondary virtual file server storing secondary copies of the user files* (Witte, col. 2, lines 49-65), *the method comprising*:

replicating changes to the user files from the primary file server to the secondary copies of the user files in the secondary virtual file server during user file access at the active site (Witte, col. 7, lines 8-20); *and*

during the replication of the changes to the user files from the primary file server to the secondary virtual file server, creating at the disaster recovery site a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a group consistent state of the user files in the secondary virtual file server (Witte, col. 7, lines 8-20, where each snap-shot state is consistent and allows a live version with seamless failover, col. 12, lines 40-54).

As per claim 21, Witte discloses *a disaster recovery system comprising: a primary file server at an active site; and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files that have been*

replicated from the primary file server to the disaster recovery site (Witte, col. 11, lines 47-61), *the secondary virtual file server needing resources including network interfaces and file system mounts at the disaster recovery site for providing user access at the disaster recovery site* (Witte, col. 7, lines 52-31), *wherein the disaster recovery system is programmed for responding to a request from a system administrator* (Witte, col. 12, line 12, where a system administrator is responsible for setting up the recovery system) by executing the determining methods as described in the previous rejection of claim 1 above, which are rejected under the same grounds when incorporated into this system, which is also disclosed by Witte.

As per claims 22, 23, 24, 25, 27, and 30, Witte discloses the system from which these dependent claims are derived as shown in the rejection of claim 21. These dependent claims merely provide a system for executing the additional methods of claims 2, 3, 4, 5, 7, and 10, and as such is rejected under the same grounds as applied respectively to claims 2, 3, 4, 5, 7, and 10 above.

As per claim 34, Witte discloses *a disaster recovery system comprising: a primary file server at an active site; and a secondary virtual file server at a disaster recovery site remote from the active site, the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site* (Witte, col. 11, lines 47-61); wherein the disaster recovery system is programmed for the maintaining methods as described in the previous rejection of claim 15 above, which are rejected under the same grounds when incorporated into this system, which is also disclosed by Witte.

As per claim 41, Witte discloses *a disaster recovery system comprising a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site* (Witte, col. 11, lines 47-61), *the primary file server storing a collection of user files, and the secondary virtual file server storing secondary copies of the user files* (Witte, col. 2, lines 49-65), *wherein the system is programmed for replicating changes to the user files from the primary file server to the secondary copies of the user files in the secondary virtual file server during user file access at the active site* (Witte, col. 7, lines 8-20), *and wherein the disaster recovery site is programmed for creating at the disaster recovery site a series of snapshot copies of the secondary virtual file server during the replication of the changes to the user files from the primary file server to the secondary virtual file server, each of the snapshot copies providing a group consistent state of the user files in the secondary virtual file server* (Witte, col. 7, lines 8-20, where each snap-shot state is consistent and allows a live version with seamless failover, col. 12, lines 40-54).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8, 9, 16, 17, 19, 28, 29, and 35-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Witte in view of Olson et al., United States Patent number 7, 069,468, filed June 28, 2002.

As per claim 8, Witte discloses *the method as claimed in claim 1, wherein a network client accessing the primary file server at the active site detects a failure of the primary file server to respond to a file access request* (Witte, col. 12, lines 7-18, where the administrator is the detecting network client) and in response to this detecting *the network client redirects the file access request to the disaster recovery site* (Witte, col. 12, lines 22-35). Witte fails to disclose this detection occurring due to a lack of timely response.

Olson discloses detecting a failure due to lack of a timely response (Olson, col. 23, lines 48-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include the timer of Olson in the methods of Witte.

This would have been obvious because Witte discloses an ability to detect the failure of the primary system (Witte, col. 12, lines 7-8), but fails to detail how such a detection might occur. Olson provides an obvious method for monitoring the health of a process, such as the filer of Witte (Olson, col. 23, lines 47-55), which would satisfy this deficiency of a detection method in Witte.

As per claim 9, Witte and Olson further disclose *the method as claimed in claim 8, wherein the network client accesses the primary file server using a CIFS connection* (Witte, col. 8, lines 15-16), *and the network client detects the failure of the primary file server to respond to the file access request in a timely fashion* (Olson, col. 23, lines 47-55) a*nd redirects the file access request to the disaster recovery site without terminating the CIFS connection* (Witte, col.

12, lines 40-54, where the user transparency of the live state shows that the connection is not terminated, merely transferred).

As per claim 16, Witte discloses *the method as claimed in claim 15, wherein a network client accessing the primary file server at the active site detects a failure of the primary file server to respond to a file access request* (Witte, col. 12, lines 7-18, where the administrator is the detecting network client) and in response to this detecting *the network client redirects the file access request to the disaster recovery site* (Witte, col. 12, lines 22-35). Witte fails to disclose this detection occurring due to a lack of timely response.

Olson discloses detecting a failure due to lack of a timely response (Olson, col. 23, lines 48-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include the timer of Olson in the methods of Witte.

This would have been obvious because Witte discloses an ability to detect the failure of the primary system (Witte, col. 12, lines 7-8), but fails to detail how such a detection might occur. Olson provides an obvious method for monitoring the health of a process, such as the filer of Witte (Olson, col. 23, lines 47-55), which would satisfy this deficiency of a detection method in Witte.

As per claim 17, Witte and Olson further disclose *the method as claimed in claim 16, wherein the network client accesses the primary file server using a CIFS connection* (Witte, col. 8, lines 15-16), *and the network client detects the failure of the primary file server to respond to the file access request in a timely fashion* (Olson, col. 23, lines 47-55) *and redirects the file*

access request to the disaster recovery site without terminating the CIFS connection (Witte, col. 12, lines 40-54, where the user transparency of the live state shows that the connection is not terminated, merely transferred).

As per claim 19, Witte discloses *in a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site* (Witte, col. 2, lines 49-60), *the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site* (Witte, col. 7, lines 11-13), *a method comprising: a network client accessing the primary file server at the active site using a CIFS connection* (Witte, col. 8, lines 15-16) *and detecting a failure of the primary file server to respond to a file access request* (Witte, col. 12, lines 7-18, where the administrator is the detecting network client) and in response to this detecting, *the network client redirecting the file access request to the disaster recovery site without terminating the CIFS connection* (Witte, col. 12, lines 40-54, where the user transparency of the live state shows that the connection is not terminated, merely transferred, where the network client is the administrator, col. 12, line 12). Witte fails to disclose this detection occurring due to a lack of timely response.

Olson discloses detecting a failure due to lack of a timely response (Olson, col. 23, lines 48-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include the timer of Olson in the methods of Witte.

This would have been obvious because Witte discloses an ability to detect the failure of the primary system (Witte, col. 12, lines 7-8), but fails to detail how such a detection might occur. Olson provides an obvious method for monitoring the health of a process, such as the filer of Witte (Olson, col. 23, lines 47-55), which would satisfy this deficiency of a detection method in Witte.

As per claim 28, Witte discloses *the system as claimed in claim 21, which includes a network client programmed to detect a failure of the primary file server to respond to a file access request* (Witte, col. 12, lines 7-18, where the administrator is the detecting network client) and in response to this detecting the network client is programmed *to redirect the file access request to the disaster recovery site* (Witte, col. 12, lines 22-35). Witte fails to disclose this detection occurring due to a lack of timely response.

Olson discloses detecting a failure due to lack of a timely response (Olson, col. 23, lines 48-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include the timer of Olson in the methods of Witte.

This would have been obvious because Witte discloses an ability to detect the failure of the primary system (Witte, col. 12, lines 7-8), but fails to detail how such a detection might occur. Olson provides an obvious method for monitoring the health of a process, such as the filer of Witte (Olson, col. 23, lines 47-55), which would satisfy this deficiency of a detection method in Witte.

As per claim 29, Witte and Olson further disclose *the system as claimed in claim 28, wherein the network client is programmed for accessing the primary file server using a CIFS connection* (Witte, col. 8, lines 15-16), *and for detecting the failure of the primary file server to respond to the file access request in a timely fashion* (Olson, col. 23, lines 47-55) a*nd redirecting the file access request to the disaster recovery site without terminating the CIFS connection* (Witte, col. 12, lines 40-54, where the user transparency of the live state shows that the connection is not terminated, merely transferred).

As per claim 35, Witte discloses *the system as claimed in claim 34, which includes a network client programmed for accessing the primary file server at the active site and for detecting a failure of the primary file server to respond to a file access request* (Witte, col. 12, lines 7-18, where the administrator is the detecting network client) and in response to this detecting programmed for *redirecting the file access request to the disaster recovery site* (Witte, col. 12, lines 22-35). Witte fails to disclose this detection occurring due to a lack of timely response.

Olson discloses detecting a failure due to lack of a timely response (Olson, col. 23, lines 48-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include the timer of Olson in the methods of Witte.

This would have been obvious because Witte discloses an ability to detect the failure of the primary system (Witte, col. 12, lines 7-8), but fails to detail how such a detection might occur. Olson provides an obvious method for monitoring the health of a process, such as the

filer of Witte (Olson, col. 23, lines 47-55), which would satisfy this deficiency of a detection method in Witte.

As per claim 36, Witte and Olson further disclose *the system as claimed in claim 35, wherein the network client is programmed for accessing the primary file server using a CIFS connection* (Witte, col. 8, lines 15-16), *and upon detecting the failure of the primary file server to respond to the file access request in a timely fashion* (Olson, col. 23, lines 47-55) *for redirecting the file access request to the disaster recovery site without terminating the CIFS connection* (Witte, col. 12, lines 40-54, where the user transparency of the live state shows that the connection is not terminated, merely transferred).

As per claim 37, Witte and Olson further disclose the system as claimed in claim 36, wherein the disaster recovery site is programmed for producing and storing a series of snapshot copies of the secondary virtual file server, each of the snapshot copies providing a consistent state for the secondary virtual file server (Witte, col. 7, lines 8-20).

As per claim 38, Witte discloses *in a disaster recovery environment including a primary file server at an active site and a secondary virtual file server at a disaster recovery site remote from the active site* (Witte, col. 2, lines 49-60), *the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site* (Witte, col. 7, lines 11-13), *a system comprising: a network client accessing the primary file server at the active site using a CIFS connection* (Witte, col. 8, lines 15-16) *and detecting a failure of the primary file server to respond to a file access request* (Witte, col. 12, lines 7-18, where the administrator is the detecting network client) and in response to this detecting, *the*

network client redirecting the file access request to the disaster recovery site without terminating the CIFS connection (Witte, col. 12, lines 40-54, where the user transparency of the live state shows that the connection is not terminated, merely transferred, where the network client is the administrator, col. 12, line 12). Witte fails to disclose this detection occurring due to a lack of timely response.

Olson discloses detecting a failure due to lack of a timely response (Olson, col. 23, lines 48-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include the timer of Olson in the methods of Witte.

This would have been obvious because Witte discloses an ability to detect the failure of the primary system (Witte, col. 12, lines 7-8), but fails to detail how such a detection might occur. Olson provides an obvious method for monitoring the health of a process, such as the filer of Witte (Olson, col. 23, lines 47-55), which would satisfy this deficiency of a detection method in Witte.

As per claim 39, Witte discloses *a disaster recovery system comprising: a primary file server at an active site; a secondary virtual file server at a disaster recovery site remote from the active site* (Witte, col. 2, lines 49-60), *the secondary virtual file server including a collection of files being replicated from the primary file server to the disaster recovery site* (Witte, col. 7, lines 11-13); *and at least one network client programmed for accessing the primary file server at the active site using a CIFS connection* (Witte, col. 8, lines 15-16) *and detecting a failure of the primary file server to respond to a file access request* (Witte, col. 12, lines 7-18, where the

administrator is the detecting network client) and in response to this detecting, *the network client redirecting the file access request to the disaster recovery site without terminating the CIFS connection* (Witte, col. 12, lines 40-54, where the user transparency of the live state shows that the connection is not terminated, merely transferred, where the network client is the administrator, col. 12, line 12). Witte fails to disclose this detection occurring due to a lack of timely response.

Olson discloses detecting a failure due to lack of a timely response (Olson, col. 23, lines 48-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include the timer of Olson in the methods of Witte.

This would have been obvious because Witte discloses an ability to detect the failure of the primary system (Witte, col. 12, lines 7-8), but fails to detail how such a detection might occur. Olson provides an obvious method for monitoring the health of a process, such as the filer of Witte (Olson, col. 23, lines 47-55), which would satisfy this deficiency of a detection method in Witte.

As per claim 40, Witte and Olson further disclose *the disaster recovery system as claimed in claim 39, wherein said at least one network client includes a CIFS redirection agent for passing CIFS requests from said at least one network client to the primary file server* (Witte, col. 12, lines 7-18, where the administrator is the network client), *the CIFS redirection agent having a timer for detecting the failure of the primary file server to respond to the file access request in a timely fashion* (Olson, col. 23, lines 47-55, where a timer is used to detect failure, and Witte, col. 12, lines 7-18, where the administrator is active in the failure detection), *and wherein the*

primary file server includes a CIFS connection maintenance agent for ensuring that a timely response to each CIFS request is returned to said at least one network client, the CIFS connection maintenance agent having a timer for determining whether the CIFS connection maintenance agent needs to return a response to said each CIFS request for maintaining the CIFS connection (Witte, col. 8, lines 15-16, where if the filers are CIFS type systems, the administrator of col. 12, lines 7-18, would be a CIFS connection maintenance agent acting to ensure the connection is properly maintained, col. 12, lines 7-54).

Allowable Subject Matter

Claims 6 and 26 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 11, 12, 13, 14, 31, 32, and 33 are allowable.

Claims 11 and 31 are allowable for including the limitations, when taken within the context of the claims as a whole, of "*upon finding that there are insufficient network interfaces and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site once the configuration change would be made to the primary file server, providing an operator with a list of missing resources or discrepancies, and receiving from the operator a choice of termination or configuration change*";

Claims 12 and 32 are allowable for including the limitations, when taken within the context of the claims as a whole of "*upon finding that there are insufficient network interfaces*

and file system mounts at the disaster recovery site for the virtual secondary file server for providing unrestricted user access at the disaster recovery site, providing an operator with a list of missing resources or discrepancies, and receiving from the operator a choice of termination or forced failover";

And claims 13, 14, and 33 are allowable for including the limitations, when taken within the context of the claims as a whole of "*maintaining a primary copy of user mappings at the disaster recovery site and a read-only cache of the user mappings at the active site during user file access at the active site; and upon failover of user access from the primary file server at the active site to the virtual secondary server at the disaster recovery site, accessing the primary copy of user mappings at the disaster recovery site in order to continue user file access at the disaster recovery site*".

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is provided on form PTO-892

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joshua A. Lohn whose telephone number is (571) 272-3661. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Baderman can be reached on (571) 272-3644. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Joshua A Lohn
Patent Examiner
Art Unit 2114